Označení dokumentu:	**ISMS-011**
Název dokumentu:	**Politika fyzické bezpečnosti JU**
Typ dokumentu:	Interní dokument - typ B – směrnice
Určeno pro:	Všechny zaměstnance, studenty a účastníky CŽV JU, zvláště správce objektů a technologických místností a všechny specialisty ICT
Prvek normy ISO:	27001
Datum vydání:	27.6.2012
Datum účinnosti:	**1.7.2012**
Platnost do:	odvolání
Počet stran + příloh:	9 + 3
Verze:	1.0
Účel:	Ochrana aktiv JU s důrazem na fyzickou bezpečnost ICT za účelem zabránit a předcházet jejich zneužívání, ztrátám nebo neautorizovaným přístupům.
Uložení:	Portál ISMS - https://isms.jcu.cz/
Ruší dokumenty:	-
Zpracovatel:	Ing. Jana Kolářová - MIB JU
Přezkoumal:	IT manažeři, správci budov a ICT součástí JU, útvar BOZP a PO
Schválil:	RNDr. Josef Milota - ředitel ISMS a CIT

OBSAH

A. ÚVODNÍ USTANOVENÍ

CÍL PROCESU A ÚČEL

Cílem této politiky je zabránit neautorizovaným přístupům, zničení, ztrátám nebo zneužívání aktiv JU, přerušení univerzitních aktivit, předcházení krádežím, případně jiným bezpečnostním incidentům spojeným s fyzickou bezpečností. Protože je třeba nejvíce chránit data a informace JU, která se zpracovávají převážně elektronicky, směrnice se zaměřuje především na ochranu prostor s informačními a komunikačními technologiemi (ICT).

POJMY, DEFINICE A ZKRATKY

1. POJMY A DEFINICE

- **Aktiva JU** – cokoli, co má pro JU nějakou hodnotu.
- **Aktiva IT -** aktiva JU spojená s procesy zpracování dat a spadající do kategorie ICT.
- **Bezpečnostní incident -** jedna nebo více nežádoucích a neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činnosti JU a ohrožení bezpečnosti informací.
- **Elektronická požární signalizace (EPS) –** soustava požárních čidel a hlásičů vyvedených obvykle na recepci dané budovy nebo přímo na centrální pult hasičského sboru.
- **Elektronický zabezpečovací systém (EZS)** – systém čidel napojených na ústřednu EZS, který při neoprávněném vstupu do chráněného objektu/prostoru spustí alarm. Bývá napojen na **PCO** (Pult centralizované ochrany).
- **Identifikační karta (IK)** - plastová čipová bezkontaktní identifikační karta přidělovaná zaměstnancům, studentům či účastníkům CŽV a absolventům pracovištěm IPS CIT JU v rámci systému JIS, která obsahuje jejich identifikační údaje nutné pro fyzický přístup do objektů JU a přístup do vybraných IS JU. Může také obsahovat certifikáty pro přihlášení z PC do sítě JU, certifikát pro elektronický podpis, případně další údaje.
- **Hrozba** - možnost vyzrazení nebo zneužití uchovávané informace při narušení fyzické bezpečnosti.
- **Objekt -** budova nebo jiný ohraničený prostor, ve kterém se nacházejí zabezpečené oblasti.
- **Provozovatel objektu –** součást JU využívající objekt k vykonávání své činnosti a odpovědná za zajištění provozu v objektu.
- **Pult centralizované ochrany -** dispečerské pracoviště, na něž jsou připojeny střežené objekty a prostory zabezpečené EZS nebo EPS, a to prostřednictvím radiové sítě, telefonních linek nebo GSM bran. Jde o službu, která ve smluvený čas střeží určené objekty. Při vyhlášení poplachu může PCO vyslat vlastní zásahovou jednotku, zároveň zavolá Policii a kontaktuje majitele objektu. V případě požárního poplachu zavolá Hasičský záchranný sbor ČR, který má i vlastní PCO.
- **Řízený přístup** – v této směrnici se týká vstupu osob do zabezpečené oblasti, kam mají samostatný přístup pouze ti, kteří k tomu mají povolení a jsou uvedeni v seznamu osob s oprávněným vstupem.
- **Správce zabezpečené oblasti** – obvykle bezpečnostní správce, správce sítě či správce ICT součásti JU pověřený vedoucím součásti JU či útvaru provozující zabezpečenou oblast, který odpovídá za její ochranu, přiděluje práva přístupu pro další osoby a řídí a eviduje vstup servisních organizací.
- **Technický prostředek** - bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje vstup nebo oznamuje narušení ochrany objektu či zabezpečené oblasti.
- **Utajované či citlivé informace** - takové informace, které vynesením, zdokumentováním nebo zničením nepovolanou osobou mohou vážně ohrozit zájmy vlastníka těchto informací.
- **Zabezpečená oblast (ZO)** – stavebně ohraničený prostor uvnitř objektu, kde se zpracovávají nebo ukládají data, zejména pak citlivé či utajované informace. Jsou to technologické místnosti se zařízeními ICT zajišťující provoz IS, zálohování dat a dodávky elektrické energie, digitální telefonní a komunikační zařízení, síťové komponenty, prostory pro archivaci médií, případně jiná technologie.

2. ZKRATKY

- **BOZP** – Bezpečnost a ochrana zdraví při práci.
- **CIT –** Centrum informačních technologií – celoškolské pracoviště JU.
- **CŽV** – celoživotní vzdělávání.
- **EPS –** viz **Elektronická požární signalizace**.
- **EZS –** viz **Elektronický zabezpečovací systém**.
- **ICT** (Information and Communication Technologies) – Informační a komunikační technologie - zahrnují veškeré technologie používané pro komunikaci a práci s informacemi.
- **IK –** viz **Identifikační karta**.
- **IPS** – Identifikační a přístupový systém – pracoviště CIT, které na JU provozuje a spravuje JIS a další IS.

- **IS** – Informační systém = systém pro sběr, udržování, zpracování a poskytování informací a dat pomocí počítačů.
- **ISMS** (Information Security Management System) – Systém řízení bezpečnosti informací.
- **IT** (Information technology) – Informační technologie - zjednodušeně řečeno počítače a vše co s nimi souvisí.
- **ITM** – IT manažer, který zajišťuje IT služby své součásti (fakulty, ústavu).
- **JIS** - Jednotný identifikační systém JU, který spravuje a udržuje pracoviště IPS CIT.
- **JU** – Jihočeská univerzita v Českých Budějovicích.
- **KS** – Kamerový systém.
- **LS PC -** lokální správce počítačů na každé součásti JU.
- **MIB –** Manažer informační bezpečnosti JU.
- **PC** (Personal Computer) – osobní počítač ve vlastnictví JU. Není-li v textu explicitně uveden konkrétní typ počítače, zahrnuje i přenosné počítače typu notebook (NB) či netbook.
- **PCO -** viz pojem **Pult centralizované ochrany.**
- **PO –** Požární ochrana.
- **UPS** (Uninterruptible Power Supply) - nepřerušitelný zdroj energie = zařízení nebo systém, který zajišťuje souvislou dodávku elektřiny pro zařízení, která nesmějí být neočekávaně vypnuta.
- **ZO** – viz pojem **Zabezpečená oblast**.

ODPOVĚDNOSTI A PRAVOMOCI

Správce zabezpečené oblasti (technologické místnosti):

- udržuje aktuální seznam osob, které mají oprávnění ke vstupu do ZO na základě předchozího schválení odpovědným vedoucím pracoviště
- přiděluje jim přístupový kód pro EZS (je-li instalován) a zároveň je poučí o povinnosti zakódování při odchodu ze ZO.
- jsou-li specifické požadavky na reakci ostrahy, PCO, EZS či EPS, předá je správci budovy, aby o nich informoval příslušné subjekty
- pokud jsou instalována v ZO zařízení jiných organizací, zajistí jejich označení názvem externí firmy
- závažná porušení fyzické bezpečnosti ZO jsou považována za bezpečnostní incident (BI), a proto je ihned řeší spolu s přímým nadřízeným a nahlásí tento BI manažeru informační bezpečnosti JU
- min. 1x ročně kontroluje funkčnost opatření fyzické bezpečnosti ZO.

Zaměstnanec, student nebo účastník CŽV JU:

- neprodleně informuje recepci, správce budovy nebo ZO (viz příloha 2 – „*ISMS-011-P2_Zabezpečené oblasti a správc*i“), zjistí-li poruchy rozvodu energií či jakékoli narušení fyzické bezpečnosti kdekoli v objektech JU
- nevstupuje samostatně do prostor ZO, nemá-li k tomu oprávnění, i kdyby se taková možnost naskytla
- chrání zařízení a pomůcky, obzvláště prostředky ICT JU jemu svěřené či poskytnuté k pracovním nebo studijním účelům
- nemanipuluje se zařízeními ICT, k nimž nemá oprávnění (přemísťování, opravy apod.)
- zkontroluje uzavření oken a dveří při odchodu z kanceláře (zaměstnanec).

Další odpovědnosti jsou součástí dokumentu.

ZMĚNY OPROTI PŮVODNÍ VERZI

Toto je druhá verze 1.0 dokumentu.
Změna oproti první verzi – kapitola 3.6. aktualizováno číslo dokumentu “Opatření rektora“.

B. POPIS

1. FYZICKÁ BEZPEČNOST OBJEKTŮ

1.1. OBECNÁ PRAVIDLA

Fyzická ochrana majetku a zdrojů je důležitým aspektem bezpečnostní strategie každé organizace. Ať už jde o bezpečnost zaměstnanců, studentů a účastníků CŽV, zabezpečení dat a systémů nebo ochranu klíčových zařízení.

- Objekty JU jsou většinou volně přístupné veřejnosti, studentům, zaměstnancům a účastníkům CŽV. Některé mají recepci či vrátnici, která pak poskytuje určité služby uvedené v provozním řádu budovy.
- JU využívá i budovy v pronájmu, na něž se pak vztahují také pravidla fyzické bezpečnosti pronajímatele.
- Přístup do některých budov či vnitřních prostorů JU je řízen identifikační kartou, kterou vydává a oprávnění ke vstupu nastavuje pracoviště IPS CIT JU.
- Zvýšení fyzické ochrany musí být věnováno technologickým místnostem s ICT (servery, aktivní síťové prvky, záložní zdroje, zálohovací zařízení apod.), dále nazývanými **zabezpečená oblast** (**ZO**). Jejich zabezpečení je popsáno v kapitole 3. níže.
- Při narušení bezpečnosti objektu či ZO je zaměstnanec, student i účastník CŽV, který narušení zjistí, povinen toto neprodleně nahlásit správci objektu, ZO nebo obsluze recepce, případně přímo děkanátu fakulty, aby byla zajištěna náprava a přijato vhodné opatření. Kontakty na správce ZO a objektů JU jsou uvedeny v příloze 2 této směrnice, viz *ISMS-011-P2_ Zabezpečené oblasti a správci*.

1.2. PROVOZNÍ ŘÁD BUDOVY

Objekt JU, v němž jsou umístěna aktiva ICT JU, má vypracován Provozní řád budovy, který zpravidla obsahuje:

- přístupy do objektu v době provozu a mimo provoz
- informace o použití identifikačních karet a JIS – přístupový systém (jsou-li využívány)
- pohyb osob v objektu
- kniha návštěv (existuje-li recepce)
- ochrana majetku
- požární ochrana, EPS, ev. odkaz na Opatření rektora týkající se PO
- informace o EZS (je-li v budově instalován)
- informace o kamerovém systému (je-li instalován)
- zajištění poslucháren a počítačových učeben – pokud v objektu existují
- kontakty na správce objektu
- event. další potřebné informace v závislosti na typu a vybavení objektu.

1.3. POKYNY PRO RECEPCI ČI VRÁTENSKOU SLUŽBU

V objektech, kde existuje recepce, mají její pracovníci k dispozici pokyny popisující nezbytné náležitosti pro provoz objektu. Pokud provoz zajišťuje externí firma, mohou být tyto pokyny přílohou smlouvy s ní uzavřenou. Jde o upřesňující informace, z nichž některé mohou být i součástí Provozního řádu budovy JU:

- režim manipulace s klíči - vydávání, řízený přístup k rezervním klíčům, záznamy o vydání apod.
- zapůjčení náhradní přístupové karty – do jakých prostor, evidence výpůjček v listinné formě atd.
- pokyny pro EZS – aktivace, deaktivace, oprávnění
- pokyny pro EPS – popis úkonů v případě signalizace
- popis obsluhy kamerového systému
- kontakty na správce objektu, firem poskytujících služby EZS a EPS atd.

1.4. KAMEROVÝ SYSTÉM (KS)

Na JU v Českých Budějovicích je instalován celouniverzitní kamerový systém, který monitoruje prostory a zařízení za účelem zajištění ochrany majetku JU. Přístup k záznamům tohoto KS má vedoucí pracoviště IPS CIT JU, ředitel CIT a jím pověření pracovníci součástí JU, kteří spravují jednotlivé úseky KS.

Záznamy z kamerového systému jsou informace typu C – důvěrné, a tak je s nimi i nakládáno. Podléhají zákonu č.101/2000 Sb. o ochraně osobních údajů. Předat je lze pouze výhradně státním orgánům činným v trestním řízení či Policii ČR, a to pouze osobně. Kamerové záznamy mohou být ze zákona uchovávány pouze po dobu nezbytně nutnou.

Doplňující informace ke KS JU jsou uvedeny v *Opatření ředitele CIT 2/2007 – Nakládání s daty získanými kamerovým systémem.*

2. POČÍTAČOVÉ UČEBNY A LABORATOŘE

Jde o místnosti sloužící studentům či účastníkům CŽV k výuce či individuálnímu studiu, které jsou vybavené větším množstvím počítačů, audiovizuálními nebo jinými komponentami ICT, a je proto také nutná jejich zvýšená fyzická ochrana.

Vhodným řešením je vstup pomocí identifikační karty nebo přítomnost správce učebny či vyučujícího v době provozu učebny.

Fyzické zabezpečení učeben je plně v kompetenci jejího provozovatele, tj. součásti JU. Využít lze stejné zabezpečovací prvky jako u ZO – viz kapitola 3. Je doporučeno, aby provoz učebny byl upraven vlastním provozním řádem.

3. FYZICKÁ OCHRANA ZABEZPEČENÝCH OBLASTÍ (ZO)

Do této oblasti spadají všechny technologické místnosti, kde jsou umístěny servery, aktivní komponenty počítačových sítí, telekomunikační ústředny, zálohovací mechaniky, UPS či jiná technologická zařízení. Jde o prostory, kde se zpracovávají informace a data všeho druhu potřebná pro chod JU nebo její součásti. Proto je nutná jejich zvýšená ochrana.

Je doporučeno v rámci možností součásti JU umístit všechna výše jmenovaná zařízení ICT do jedné či více ZO, kde jsou dostatečně chráněna uplatněním dále popsaných zásad a opatření. V případě nově budovaných objektů JU je třeba toto zohlednit již při tvorbě projektu.

Seznam zabezpečených oblastí (technologických místností) JU je uveden v příloze 2 tohoto dokumentu – viz „***ISMS-011-P2_Zabezpečené oblasti a správci***“ a navíc také dostupný na portále https://isms.jcu.cz/ ve složce ***Kontakty***.

3.1. ZÁKLADNÍ ZAJIŠTĚNÍ ZABEZPEČENÉ OBLASTI

Zabezpečené oblasti jsou chráněny kombinací základních opatření fyzické bezpečnosti. Jde o tyto bezpečnostní prvky:

- vstupní dveře mají nainstalován bezpečnostní zámek s koulí, a pokud jsou prosklené, musí být opatřeny bezpečnostní fólií
- má-li ZO okna v přízemí nebo snadno přístupná zvenku, jsou opatřena kovovou mříží nebo bezpečnostní fólií, případně čidly EZS
- v ZO je instalováno požární čidlo s řídící jednotkou signalizující požár buď na mobil správce ZO, budovy, PCO nebo přímo na hasičský záchranný sbor
- v bezprostřední blízkosti vstupu či uvnitř ZO je umístěn hasicí přístroj odpovídajícího typu
- kabely vedoucí vně a dle možnosti i uvnitř ZO jsou vedeny v plastových či kovových žlabech
- racky (normované skříně pro přehlednou montáž různých elektrických a elektronických zařízení a jejich kabeláže) umístěné mimo ZO nebo v učebnách jsou uzamčené a přístupné jen určeným správcům.

Pokud některé ZO nesplňují tyto základní požadavky, pak součásti JU, které je provozují, implementují výše uvedené ochranné prvky nejpozději do konce roku 2013.

3.2. DOPORUČENÁ BEZPEČNOSTNÍ OPATŘENÍ

Tato opatření jsou volitelná, o jejich zavedení rozhoduje každá součást JU provozující ZO a závisí na hodnotě aktiv umístěných v ZO a na finančních možnostech součástí. U nově vybudovaných prostorů je doporučováno využít kromě základních i další ochranné prvky:

- mechanické zábranné prostředky – bezpečnostní a protipožární dveře, čidla oken a dveří
- EZS – detektory pohybu
- systémy pro kontrolu vstupů – snímače identifikačních karet či biometrických údajů
- racky umístěné uvnitř ZO
- kamerové systémy, případně další.

3.3. DALŠÍ BEZPEČNOSTNÍ ZÁSADY

Jejich implementace je v kompetenci jednotlivých součástí JU a závisí na jejich možnostech a skutečnosti, zda jde o nové či již existující prostory, kde by finanční náročnost úprav nebyla adekvátní hodnotě

umístěných aktiv ICT. Zdrojem pro odhad této hodnoty je evidence aktiv ICT každé součásti na portále ISMS.

Je doporučeno mít:

- servery prostorově oddělené od zálohovacích zařízení a mechanik
- archiv zálohovacích médií umístěný v samostatné chráněné místnosti s řízeným přístupem nebo použít geograficky oddělené datové úložiště s odpovídajícím zabezpečením
- důležitá technologická zařízení napojená na náhradní elektrický zdroj (UPS) s pravidelnou údržbou a záznamy o ní, např. v provozním deníku UPS či napojeného serveru vedeného na portálu https://isms.jcu.cz/ ve složce Aktiva IT u příslušné součásti
- instalovanou klimatizaci revidovanou dle doporučení výrobce.

V zabezpečených oblastech, PC učebnách a laboratořích je zakázáno:

- pořizovat obrazové záznamů neoprávněnými osobami (netýká se kamerového systému)
- manipulovat se zařízením bez příslušného oprávnění
- jíst a kouřit.

3.4. POHYB OSOB V ZABEZPEČENÝCH OBLASTECH

- Seznam osob, které mohou vstupovat do zabezpečené oblasti, je uložen u správce ZO nebo správce budovy, kteří vydávají oprávnění ke vstupu do těchto prostor na základě předchozího schválení odpovědným vedoucím pracoviště, jež ZO provozuje.
- Pro evidenci osob s oprávněním vstupu slouží příloha 3 této politiky - viz ***„ISMS-011-P3_ Seznam osob oprávněných ke vstupu do ZO“***. *B*ezpečnostní správce každé součásti JU, která má vlastní technologickou místnost/ti musí mít tento aktuální seznam k dispozici pro případ řešení bezpečnostního incidentu nebo auditu ISMS, a to pro každou ZO, nejsou-li přístupy shodné do všech ZO součásti JU.
- Je-li vstup do ZO řízen identifikační kartou (IK), oprávnění nastavuje vedoucí pracoviště IPS CIT JU na základě schválení vedoucím pracoviště, jež ZO provozuje. IPS CIT vede aktuální seznam osob s tímto oprávněním.
- Samostatný vstup a pohyb jiných než oprávněných a evidovaných osob je zakázán.
- Zaměstnanci servisních organizací mohou v ZO vykonávat činnost pouze za dohledu správce ZO, objektu nebo jimi pověřených osob oprávněných ke vstupu do ZO.
- Správce ZO, objektu či oprávněná osoba, která umožnila externí firmě vstup do ZO, zaeviduje tuto návštěvu do formuláře “ ***ISMS-011-P1_Evidence návštěv servisních zásahů***“ – viz příloha P1 této směrnice, který je umístěn v listinné podobě v každé ZO, případně může být v kopii veden i elektronicky správcem ZO.
- V případě výskytu mimořádné události (požáru, záplavy, havárie vody, zemětřesení, útoku apod.) může vlastník budovy se ZO a jím pověřené osoby (ostraha, zaměstnanci správce budovy), pokud je to nutné pro odvrácení ohrožení životů nebo zdraví osob nebo poškození budovy a dalšího majetku, použít duplikát klíče pro vstup do ZO. O události musí být bez zbytečného prodlení informován správce ZO.

3.5. MANIPULACE S KLÍČI

- Klíče k zabezpečené oblasti jsou jednoznačně označeny, ukládají se způsobem, který umožňuje kontrolu jejich použití a jejich výdej podléhá evidenci. S klíči disponuje správce objektu nebo správce zabezpečené oblasti.
- Pokud jsou klíče trvale přiděleny správcům ICT, kteří mají oprávnění vstupu do ZO, musí mít správce objektu nebo správce ZO, který klíče přiděloval, aktuální seznam jmen těchto zaměstnanců s datem vydání klíče a podpisem přebírajícího.
- V případě předávání klíčů od ZO přes recepci, musí být i tam k dispozici seznam oprávněných osob a písemný záznam o zapůjčení klíče (komu, kdy půjčen a vrácen).
- Zabezpečená oblast musí být v době nepřítomnosti osob, které do ní mají povolen vstup, uzamčena.
- Ztráta klíčů musí být neprodleně oznámena správci zabezpečené oblasti, který zajistí nápravu (např. výměnu vložky).

3.6. POUŽITÍ IDENTIFIKAČNÍCH KARET (IK)

- Podrobné pokyny pro správu IK jsou v příloze 1 Opatření rektora č. R325/2016 k uplatnění a zavádění jednotného identifikačního a přístupového systému na JU.
- Uživatel JU - vlastník IK, na kterou bylo vydáno povolení ke vstupu do ZO, je povinen neprodleně po zjištění ztráty IK toto nahlásit pracovišti IPS CIT JU. Karta bude zneplatněna a zablokována.

3.7. POŽADAVKY NA ZABEZPEČENOU OBLAST

- Stěny, podlahy a stropy ZO v nových objektech mají zděnou stavební konstrukci.

- Mechanické zábranné prostředky nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup.
- Okna, dveře a další uzávěry splňují v nových objektech požadavky bezpečnostní třídy 4 podle *ČSN P ENV 1627.*

3.8. OSTRAHA OBJEKTU SE ZO

- Stanovení ostrahy objektu se zabezpečenou oblastí je závislé na vnitřním provozu a míře předpokládaného rizika a je v kompetenci vedoucího součásti JU.
- Je-li ZO zajištěna sama o sobě alespoň základními opatřeními fyzické bezpečnosti (viz bod 3.1.), není ostraha vlastního objektu nutná.

3.9. ELEKTRICKÝ ZABEZPEČOVACÍ SYSTÉM (EZS)

Je-li ZO chráněna EZS, splňuje požadavky *ČSN EN 50131-1 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy*. Pohybová čidla jsou pak napojena do ústředny EZS a signalizace vyvedena buď na stanoviště určené pro výkon ostrahy, na mobil určeného správce nebo na PCO.

3.10. ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE (EPS)

V ZO jsou instalovány požární hlásiče zapojené do ústředny EPS nebo EZS. Signál poplachu je vyveden buď na stanoviště určené pro výkon ostrahy nebo na mobil správce ZO či budovy, případně na PCO.

3.11. ÚKLID ZABEZPEČENÝCH OBLASTÍ

Úklid v ZO se neprovádí pravidelně denně jako v ostatních kancelářích, ale na požádání správce ZO a pouze za jeho dohledu. Úklidová služba nesmí mít samostatný vstup do ZO, tedy nevlastní ani jí nejsou dostupné klíče od ZO či identifikační karta ke vstupu.

3.12. OVĚŘOVÁNÍ ÚČINNOSTI OPATŘENÍ

Ověření, zda jednotlivá použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají pravidlům a zásadám uvedeným v této směrnici, provádí správce zabezpečené oblasti nebo bezpečnostní správce součásti JU průběžně, nejméně však jednou ročně. V případě nesouladu informuje svého nadřízeného s návrhem na řešení nápravy.

3.13. CERTIFIKOVANÁ ZAŘÍZENÍ

Doporučená certifikovaná zařízení pro zajištění fyzické bezpečnosti jsou publikována v seznamech těchto zařízení vydaných Národním bezpečnostním ústavem a dostupných na portálu www.nbu.cz.

Odkazy na normy související s fyzickou bezpečností ZO jsou uvedeny v oddílu C. tohoto dokumentu.

C. ZÁVĚREČNÁ USTANOVENÍ

Kontrolou dodržování této směrnice jsou pověřeni IT manažeři součástí JU, bezpečnostní správci, správci zabezpečených oblastí, případně zaměstnanci pověření ředitelem CIT a ISMS JU. Porušování cílů a zásad definovaných v této a další návazné dokumentaci ISMS zaměstnancem, studentem či účastníkem CŽV JU poškozuje dobré jméno a zájmy univerzity a může být považováno za porušování pracovních nebo studijních povinností.

SEZNAM PŘÍLOH

Označení přílohy	Název přílohy
ISMS-011-P1	Evidence návštěv-servisní zásahy
ISMS-011-P2	Zabezpečené oblasti a správci
ISMS-011-P3	Seznam osob oprávněných ke vstupu do ZO

SOUVISEJÍCÍ DOKUMENTY (platné v době vydání směrnice)

Označení dokumentu	Název dokumentu
ČSN EN ISO 9001	Systémy managementu jakosti
ČSN ISO/IEC 27001	Systém řízení bezpečnosti informací - ISMS
ČSN ISO/IEC 17799	Soubor postupů pro řízení bezpečnosti informací
ČSN EN 50131-1	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy
ČSN EN 1627 (746001)	Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace
Vyhláška č. 523/2005 Sb.	Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi
Vyhláška č. 528/2005 Sb.	Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků
Zákon 101/2000 Sb.	O ochraně osobních údajů a pozdější předpisy
R325/2016	Opatření rektora k uplatnění a zavádění jednotného identifikačního a přístupového systému na JU
R 202/2012	Opatření rektora JU ke stanovení organizace požární ochrany na JU
R 131/2009	Opatření rektora JU – Provozní řád REK a FF
R 95/2007	Opatření rektora - Užívání PC, SW, NET
ŘCIT 2/2007	Opatření ředitele CIT – Nakládání s daty získanými kamerovým systémem
ISMS-001	Politika ISMS JU
ISMS-002	Celková bezpečnostní politika JU
ISMS-003	Provozní postupy
ISMS-007	Správa a bezpečnost provozu počítačů